Amendments to the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application:

Listing of Claims:

1-16. (Canceled)

17. (New) An information security policy evaluation system comprising:

a first information processing apparatus located at a first site;

a second information processing apparatus located at a second site;

a third information processing apparatus located at a third site; and

a fourth information processing apparatus located at a fourth site,

the first to fourth information processing apparatuses in data communication with each other,

wherein the second information processing apparatus having a treated threat data storage section for storing treated threat data, the treated threat data being data indicating a threat which can be countered by an information security policy operating at the second site,

the third information processing apparatus having a threat data storage section for storing threat data which is data indicating a previous occurrence of a threat, and a loss amount data storage section for storing loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat,

the second information processing apparatus having a treated threat data transmission section for transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus having a threat data transmission section for attaching the loss amount data to the threat data and transmitting the threat data to the first information processing apparatus,

the first information processing apparatus having a treated threat data reception section for receiving the treated threat data and a threat data reception section for receiving the loss amount data as well as the threat data,

the first information processing apparatus having a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and the treated threat data, and a loss amount data storage section for storing the received loss amount data,

the first information processing apparatus having an effective treated threat data extraction section for extracting a piece of treated threat data to which there is a piece of threat data corresponding in the threat data received by the threat data reception section, out of the treated threat data received by the treated threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted treated threat data is described,

the fourth information processing apparatus having a compensation amount storage section for storing a compensation amount of insurance which an organization operating the second site has taken out and which compensates a loss occurring in a case where damage due to a threat is suffered,

the first information processing apparatus having an evaluation data transmission section for transmitting the evaluation data generated by the evaluation data generation section to the fourth information processing apparatus,

the fourth information processing apparatus having an evaluation data reception section for receiving the evaluation data,

the fourth information processing apparatus having a compensation amount setting section for resetting the stored compensation amount to the compensation amount determined in accordance with the evaluation data received by the evaluation data reception section.

18. (New) The information security policy evaluation system according to claim 17 wherein the loss amount data storing section of the third information processing apparatus stores a monetary damage amount indicating, for said each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat.

19. (New) The information security policy evaluation system according to claim 17, wherein

the first information processing apparatus has a loss amount data storage section for storing loss amount data, the loss amount data being data which indicates, for said each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat, and

the evaluation data generation section has a consideration priority sort section for generating the evaluation data in which the threat data extracted by the untreated threat data extraction section is sorted and described in descending order of the loss amount data.

20. (New) The information security policy evaluation system according to claim 17, wherein

the threat data transmission section of the third information processing apparatus attaches the loss amount data to the threat data and transmits the loss amount data to the first information processing apparatus,

the threat data reception section of the first information processing apparatus receives the loss amount data as well as the threat data, and

the loss amount data storage section of the first information processing apparatus stores the received loss amount data.

21. (New) The information security policy evaluation system according to claim 17 wherein the third information processing apparatus has a threat data update section for updating the threat data and the threat data transmission section transmits the updated threat data to the first information processing apparatus in a case where the threat data has been updated by the threat data update section.

22. (New) An information security policy evaluation system comprising:

a first information processing apparatus located at a first site;

a second information processing apparatus located at a second site; and

a third information processing apparatus located at a third site,

a fourth information processing apparatus located at a fourth site,

the first to fourth information processing apparatuses in data communication with each other, wherein:

the second information processing apparatus has a treated threat data storage section for storing treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past, and a loss amount data storage section for storing loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat,

the second information processing apparatus has a treated threat data transmission section for transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus has a threat data transmission section for attaching the loss amount data to the threat data and transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a treated threat data reception section for receiving the treated threat data and a threat data reception section for receiving the loss amount data as well as the threat data,

the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and the treated threat data, and a loss amount data storage section for storing the received loss amount data,

the first information processing apparatus has an untreated threat data extraction section for extracting a piece of threat data to which there is no piece of treated threat data corresponding in the treated threat data received by the treated threat data reception section, out of the threat data received by the threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted threat data is described,

the fourth information processing apparatus has a compensation amount storage section for storing a compensation amount of insurance which an organization operating the second site has taken out and which compensates a loss occurring in a case where damage due to a threat is suffered,

the first information processing apparatus has an evaluation data transmission section for transmitting the evaluation data generated by the evaluation data generation section to the fourth information processing apparatus,

the fourth information processing apparatus has an evaluation data reception section for receiving the evaluation data, and

the fourth information processing apparatus has a compensation amount setting section for resetting the stored compensation amount to the compensation amount determined in accordance with the evaluation data received by the evaluation data reception section.

23. (New) The information security policy evaluation system according to claim 22 wherein the loss amount data storing section of the third information processing apparatus stores a monetary damage amount indicating, for said each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat.

24. (New) The information security policy evaluation system according to claim 22 wherein the third information processing apparatus has a threat data update section for updating the threat data and, the threat data transmission section transmits the updated threat data to the first information processing apparatus in a case where the threat data has been updated by the threat data update section.

25. (New) An information security policy evaluation system comprising:

a first information processing apparatus located at a first site;

a second information processing apparatus located at a second site; and

a third information processing apparatus located at a third site,

the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a policy data storage section for storing policy data which is data indicating an information about a security policy operated on the second site,

wherein the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

wherein the second information processing apparatus has a policy data transmission section for transmitting the policy data to the first information processing apparatus,

wherein the third information processing apparatus has a threat data transmission section for transmitting the threat data to the first information processing apparatus,

wherein the first information processing apparatus has a policy data reception section for receiving the policy data and a threat data reception section for receiving the threat data,

wherein the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and policy data indicating an effective information security policy against a threat indicated by the threat data, and

wherein the first information processing apparatus has an effective policy data extraction section for extracting a piece of policy data to which there is a piece of threat data corresponding in the threat data received by the threat data reception section, out of the policy data received by the policy data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted policy data is described.

26. (New) An information security policy evaluation system comprising:

a first information processing apparatus located on a first site;

a second information processing apparatus located on a second site; and

a third information processing apparatus located on a third site,

the first to third information processing apparatuses being capable of communicating with each other,

wherein the second information processing apparatus has a policy data storage section for storing policy data which is data indicating an information about a security policy operated on the second site,

the third information processing apparatus has a threat data storage section for storing threat data which is data indicating a threat having occurred in a past,

the second information processing apparatus has a policy data transmission section for transmitting the policy data to the first information processing apparatus,

the third information processing apparatus has a threat data transmission section for transmitting the threat data to the first information processing apparatus,

the first information processing apparatus has a policy data reception section for receiving the policy data and a threat data reception section for receiving the threat data,

the first information processing apparatus has a correspondence data storage section for storing correspondence data which is data indicating correspondence between the threat data and policy data indicating an effective information security policy against a threat indicated by the threat data, and

the first information processing apparatus has an untreated threat data extraction section for extracting a piece of threat data to which there is no piece of policy data corresponding in the policy data received by the policy data reception section, out of the threat data received by the threat data reception section, based on the correspondence data, and an evaluation data generation section for generating evaluation data in which the extracted threat data is described.

27. (New) A method of controlling an information security policy evaluation system having a first information processing apparatus located on a first site, a second information processing apparatus located on a second site, a third information processing apparatus located on a third site, a fourth information processing apparatus located on a fourth site, the first to fourth information processing apparatuses being capable of communicating with each other, the method comprising:

the second information processing apparatus storing treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus storing threat data which is data indicating a threat having occurred in a past and loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat,

the second information processing apparatus transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus attaching the loss amount data to the threat data and transmitting the threat data to the first information processing apparatus,

the first information processing apparatus receiving the treated threat data, the threat data, and the loss amount data as well as the threat data,

the first information processing apparatus storing correspondence data which is data indicating correspondence between the threat data and the treated threat data, and the received loss amount data,

the first information processing apparatus extracting a piece of treated threat data to which there is a piece of threat data corresponding in the received threat data, out of the received treated threat data based on the correspondence data, and generating evaluation data in which the extracted treated threat data is described,

the fourth information processing apparatus storing a compensation amount of insurance which an organization operating the second site has taken out and which compensates a loss occurring in a case where damage due to a threat is suffered,

the first information processing apparatus transmitting the evaluation data generated by the evaluation data generation section to the fourth information processing apparatus,

the fourth information processing apparatus receiving the evaluation data and resetting the stored compensation amount to the compensation amount determined in accordance with the evaluation data received by the evaluation data reception section.

28. (New) A method of controlling an information security policy evaluation system having a first information processing apparatus located on a first site, a second information processing apparatus located on a second site, a third information processing apparatus located on a third site, a fourth information processing apparatus located on a fourth site, the first to fourth information processing apparatuses being capable of communicating with each other, the method comprising:

the second information processing apparatus storing treated threat data, the treated threat data being data indicating a threat which an information security policy operated on the second site can counter,

the third information processing apparatus storing threat data which is data indicating a threat having occurred in a past and loss amount data, the loss amount data being data which indicates, for each piece of the threat data, a magnitude of a loss occurring in a case where damage is suffered due to a threat,

the second information processing apparatus transmitting the treated threat data to the first information processing apparatus,

the third information processing apparatus attaching the loss amount data to the threat data and transmitting the threat data to the first information processing apparatus,

the first information processing apparatus receiving the treated threat data and the loss amount data as well as the threat data,

the first information processing apparatus storing correspondence data which is data indicating correspondence between the threat data and the treated threat data and the received loss amount data

the first information processing apparatus extracting a piece of threat data to which there is no piece of treated threat data corresponding in the received treated threat data, out of the received threat data based on the correspondence data, and generating evaluation data in which the extracted threat data is described,

the fourth information processing apparatus storing a compensation amount of insurance which an organization operating the second site has taken out and which compensates a loss occurring in a case where damage due to a threat is suffered,

the first information processing apparatus transmitting the evaluation data generated by the evaluation data generation section to the fourth information processing apparatus,

the fourth information processing apparatus receiving the evaluation data and resetting the stored compensation amount to the compensation amount determined in accordance with the evaluation data received by the evaluation data reception section.